CAV 26.30 PROGRAMA CIBERSEGURIDAD INDUSTRIAL. CONVOCATORIA 2026

24 de Mayo de 2026
La SPRI (Agencia Vasca de Desarrollo Empresarial) ha hecho público el Programa Ciberseguridad Industrial 2026.

El objetivo es apoyar proyectos que incrementen de manera significativa, la ciberseguridad y la resiliencia operativa de las empresas de la CAE y de sus productos, promoviendo la mejora de sus sistemas de gestión de ciberseguridad.

Plazo presentación de solicitudes
Hasta el 23 de noviembre de 2026

Beneficiarios
Todas las empresas industriales o de servicios conexos ligados al producto-proceso industrial, que dispongan un centro de actividad en la CAE y figuren de alta en el IAE del País Vasco.

Actuaciones subvencionables
Los proyectos deberán encuadrarse en alguna de las fases relacionadas con los procesos habituales de adecuación y certificación a normativas o estándares en ciberseguridad. No es obligatorio, para una misma actuación elegible, abarcar la totalidad de las fases, ni ejecutar todas las actuaciones descritas para el caso de una misma fase. Las fases contempladas dentro del «itinerario», así como las tipologías de proyectos asociadas a cada una, que se considerarán a su vez elegibles, se detallan a continuación:
I.– Ciberseguridad en la empresa:
a) **Diagnóstico Inicial:** Proyectos orientados a analizar la situación de la empresa en materia de ciberseguridad, incluyendo auditorías, evaluación de controles y políticas existentes, así como actuaciones dirigidas a conocer el nivel de concienciación y capacitación de la plantilla.
b) **Estrategia y Planes de Acción:** Actuaciones dirigidas a definir y desarrollar la estrategia de ciberseguridad de la empresa, como planes directores de seguridad y planes de acción orientados a mejorar de forma estructurada la protección y la gestión de la ciberseguridad.
c) **Implementación de soluciones y medidas:** Proyectos destinados a implantar medidas organizativas y técnicas que refuercen la ciberseguridad y la resiliencia operativa de la empresa, abarcando desde el análisis de activos y riesgos, el gobierno de la ciberseguridad, la protección de sistemas y redes, hasta la detección, respuesta y recuperación ante incidentes.
d) **Evaluación, auditoría y certificación:** Actuaciones orientadas a la evaluación de conformidad, auditoría y certificación de la ciberseguridad de la empresa conforme a marcos y estándares reconocidos a nivel internacional.
e) **Mejora continua:** Proyectos dirigidos a la revisión, mantenimiento y renovación de certificaciones y sistemas de gestión de ciberseguridad, con el objetivo de asegurar su actualización y eficacia en el tiempo.

II. Ciberseguridad en producto (NUEVO):
a) **Seguridad del producto a lo largo de su ciclo de vida:** Proyectos orientados a implantar marcos organizativos y de proceso que aseguren la ciberseguridad del producto desde su diseño hasta su puesta en operación y mantenimiento.
b) **Diseño y desarrollo seguro de productos:** Actuaciones de consultoría dirigidas a integrar la ciberseguridad desde las fases iniciales del diseño y desarrollo del producto, incorporando criterios de seguridad por diseño, análisis de amenazas, revisión de código y validación de arquitecturas seguras.
c) **Protección de datos y gestión de vulnarabilidades:** Proyectos orientados a la implantación de mecanismos de cifrado de datos en tránsito y en reposo, autenticación y gestión segura de claves, así como a la gestión activa

de vulnerabilidades en productos.
d) **Evaluación y certificación de ciberseguridad de producto:** Actuaciones destinadas a la evaluación, verificación y certificación de la ciberseguridad de los productos conforme a normativas y estándares reconocidos.

Gastos elegibles
1. **Consultoría, ingeniería, hardware y software** y que cumplan los siguientes requisitos:
a) Devengados o facturados a partir del 1 de enero de 2026 y durante el plazo establecido para la ejecución del proyecto, que no podrá superar el de 12 meses.
b) Realizados por empresas expertas externas.
2. Para proyectos que contemplen la implantación de aplicaciones de gestión en formato tipo SAAS (Software as a Service), también podrá ser considerado como gasto elegible el coste imputable a este tipo de servicio durante un plazo máximo de 12 meses.

Naturaleza de las ayudas
1. Estas ayudas tendrán la consideración de **subvenciones a fondo perdido** y se concederán conforme al procedimiento de concesión sucesiva de las solicitudes correctamente recibidas. **Se resolverán de forma individual y ordenada** en función del momento en que haya sido completada la solicitud con toda la documentación exigida en las bases.
2. Las ayudas concedidas en aplicación de este Programa tienen la consideración de **ayudas de menor importancia o de mínimis.**

Modalidad y cuantía de las ayudas
Las ayudas se instrumentarán en forma de **subvenciones.**

El importe máximo de la subvención es de 100.000 euros por empresa beneficiaria, independientemente de que se presente uno o varios proyectos dentro del ejercicio. La ayuda cubre hasta el 60% de los gastos elegibles del proyecto.

Los gastos de consultoría y/o ingeniería deberán representar al menos el 20% de la base elegible del proyecto. De manera excepcional, esta obligación no se aplicará a los proyectos destinados a implementar productos o soluciones desarrolladas y proporcionadas por empresas que cuenten con el sello “Cybersecurity Made in Europe” de ECSO.

Pago de la ayuda
Las subvenciones serán formalizadas y entregadas por SPRI mediante **un único pago** a la entidad beneficiaria de la ayuda, tras la oportuna presentación, por parte de esta, de la solicitud de liquidación y documentación justificativa.

Ayudas sujetas al regimen de minimis.

Para más información, no duden en ponerse en contacto con nosotros (Tlf.: 943 30 90 09 **-** afm@afm.es)